

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

- 1 1. (Currently amended) A method for facilitating the delegation of
2 operations involved in providing digital signatures to a signature server, the
3 method comprising:
 - 4 allowing a user to authenticate the signature server prior to sending a
5 message to the signature server;
 - 6 receiving the message from the user at the signature server, the message
7 including an item to be signed on behalf of the user by the signature server, a user
8 identifier which identifies the user, and an application identifier which identifies
9 the application being used;
 - 10 authenticating the user at the signature server;
 - 11 determining whether the user is authorized to sign the item by
12 communicating with an authority server that is separate from the signature server;
 - 13 looking up a private key for the user at the signature server based on the
14 user identifier and the application identifier, wherein looking up a private key for
15 the user based on the user identifier and application identifier prevents a user who
16 is allowed to access a second application, but who is not allowed to access the
17 application being used, from gaining access to the application being used; and
18 signing the item with the private key for the user.
- 1 2-3 (Canceled).

1 4. (Previously presented) The method of claim 1, wherein determining
2 whether the user is authorized to sign the item involves looking up an
3 authorization for the user based upon an identifier for the user as well as an
4 identifier for an application to which the user will send the signed item.

1 5-6 (Canceled).

1 7. (Previously presented) The method of claim 1, further comprising
2 returning the signed item to the user so that the user can send the signed item to a
3 recipient.

1 8. (Original) The method of claim 1, wherein the method further
2 comprises configuring the signature server to accommodate a new user by:
3 receiving a request from an authorized entity to add the new user;
4 generating a key pair for the new user, including a new user private key
5 and a new user public key;
6 communicating with a certification authority to obtain a certificate for the
7 new user based on the key pair; and
8 storing the certificate and the key pair for the new user in a location that is
9 accessible by the signature server to enable the signature server to sign items on
10 behalf of the new user.

1 9. (Original) The method of claim 1, wherein the method further
2 comprises configuring the signature server to delete an old user by:
3 receiving a request from an authorized entity to delete the old user;
4 notifying a certification authority to revoke a certificate for the old user;
5 and

6 removing the private key for the old user from the signature server, so that
7 the signature server can no longer sign items on behalf of the old user.

1 10. (Previously presented) The method of claim 1, wherein the method
2 further comprises archiving the message and the signed item at the signature
3 server.

1 11. (Original) The method of claim 1, wherein the method further
2 comprises forwarding the signed item to an archive server in order to be archived.

1 12. (Currently amended) A computer-readable storage medium storing
2 instructions that when executed by a computer cause the computer to perform a
3 method for facilitating the delegation of operations involved in providing digital
4 signatures to a signature server, the method comprising:
5 allowing a user to authenticate the signature server prior to sending a
6 message to the signature server;
7 receiving the message from the user at the signature server, the message
8 including an item to be signed on behalf of the user by the signature server, a user
9 identifier which identifies the user, and an application identifier which identifies
10 the application being used;
11 authenticating the user at the signature server;
12 determining whether the user is authorized to sign the item by
13 communicating with an authority server that is separate from the signature server;
14 looking up a private key for the user at the signature server based on the
15 user identifier and the application identifier, wherein looking up a private key for
16 the user based on the user identifier and application identifier prevents a user who
17 is allowed to access a second application, but who is not allowed to access the
18 application being used, from gaining access to the application being used; and

19 signing the item with the private key for the user.

1 13-14 (Canceled).

1 15. (Previously presented) The computer-readable storage medium of
2 claim 12, wherein determining whether the user is authorized to sign the item
3 involves looking up an authorization for the user based upon an identifier for the
4 user as well as an identifier for an application to which the user will send the
5 signed item.

1 16-17 (Canceled).

1 18. (Previously presented) The computer-readable storage medium of
2 claim 12, wherein the method further comprises returning the signed item to the
3 user so that the user can send the signed item to a recipient.

1 19. (Original) The computer-readable storage medium of claim 12,
2 wherein the method further comprises configuring the signature server to
3 accommodate a new user by:
4 receiving a request from an authorized entity to add the new user;
5 generating a key pair for the new user, including a new user private key
6 and a new user public key;
7 communicating with a certification authority to obtain a certificate for the
8 new user based on the key pair; and
9 storing the certificate and the key pair for the new user in a location that is
10 accessible by the signature server to enable the signature server to sign items on
11 behalf of the new user.

1 20. (Original) The computer-readable storage medium of claim 12,
2 wherein the method further comprises configuring the signature server to delete an
3 old user by:
4 receiving a request from an authorized entity to delete the old user;
5 notifying a certification authority to revoke a certificate for the old user;
6 and
7 removing the private key for the old user from the signature server, so that
8 the signature server can no longer sign items on behalf of the old user.

1 21. (Previously presented) The computer-readable storage medium of
2 claim 12, wherein the method further comprises archiving the message and the
3 signed item at the signature server.

1 22. (Original) The computer-readable storage medium of claim 12,
2 wherein the method further comprises forwarding the signed item to an archive
3 server in order to be archived.

1 23. (Currently amended) An apparatus that facilitates delegating
2 operations involved in providing digital signatures, comprising:
3 a signature server;
4 an authentication mechanism that is configured to allow a user to
5 authenticate the signature server prior to sending a message to the signature server
6 a receiving mechanism within the signature server that is configured to
7 receive the message from the user, the message including an item to be signed on
8 behalf of the user by the signature server, a user identifier which identifies the
9 user, and an application identifier which identifies the application being used;
10 an authenticating mechanism configured to authenticate the user at the
11 signature server;

12 a determining mechanism configured to determine whether the user is
13 authorized to sign the item by communicating with an authority server that is
14 separate from the signature server;
15 a lookup mechanism within the signature server that is configured to look
16 up a private key for the user based on the user identifier and the application
17 identifier, wherein looking up a private key for the user based on the user
18 identifier and application identifier prevents a user who is allowed to access a
19 second application, but who is not allowed to access the application being used,
20 from gaining access to the application being used; and
21 a signing mechanism within the signature server that is configured to sign
22 the item with the private key for the user.

1 24-25 (Canceled).

1 26. (Previously presented) The apparatus of claim 23, wherein the
2 authorization mechanism is configured to determine whether the user is
3 authorized to sign the item by looking up an authorization for the user based upon
4 an identifier for the user as well as an identifier for an application to which the
5 user will send the signed item.

1 27-28 (Canceled).

1 29. (Previously presented) The apparatus of claim 23, further comprising a
2 sending mechanism within the signature server that is configured to return the
3 signed item to the user so that the user can send the signed item to a recipient.

1 30. (Original) The apparatus of claim 23, further comprising an
2 initialization mechanism that is configured to:

3 receive a request from an authorized entity to add a new user;
4 generate a key pair for the new user, including a new user private key and
5 a new user public key;
6 communicate with a certification authority to obtain a certificate for the
7 new user based on the key pair; and to
8 store the certificate and the key pair for the new user in a location that is
9 accessible by the signature server to enable the signature server to sign items on
10 behalf of the new user.

1 31. (Original) The apparatus of claim 23, further comprising a deletion
2 mechanism that is configured to:
3 receive a request from an authorized entity to delete an old user;
4 notify a certification authority to revoke a certificate for the old user; and
5 to
6 remove the private key for the old user from the signature server, so that
7 the signature server can no longer sign items on behalf of the old user.

1 32. (Previously presented) The apparatus of claim 23, further comprising
2 an archiving mechanism that is configured to archive the message and the signed
3 item at the signature server.

1 33. (Original) The apparatus of claim 23, further comprising an archiving
2 mechanism that is configured to forward the signed item to an archive server in
3 order to be archived.